My Account Was Included in a Data Breach: What Do I Do?

At least once a month, we get news that another company has been the victim of a data breach. You had signed up for an account with this company, trusting them with your username and password; maybe you even had your address or credit card number saved with your account as well. And now that data is in the hands of an attacker, who might use it for their own nefarious purposes or share it publicly on the dark web for other cybercriminals to use. That's the bad news.

The good news? You can protect yourself and keep your accounts secure, even after your information is included in a data breach!

TLDR; Now is a good time to change passwords, ensure that your passwords are both strong and unique, start using a password manager if you do not already, and start using two-factor-authentication to protect your important accounts. Keep reading to learn why, what, and how.

How can I find out if I've been affected?

There's a great site called "have I been pwned?" which aggregates the contents of data breaches so that you can check if any accounts associated with your email address have been compromised.

So head over to https://haveibeenpwned.com/ and enter in your email address. If any accounts under that email address were compromised, it will let you know "Oh no — pwned!" and provide you with a list of the breaches in which your email address was included along with additional information about each of those breaches.

Even if you weren't included in this breach, we encourage you to read on to learn more about some security best practices.

So your account was included in a breach… what now?

Being included in a breach might sound scary — but don't panic!

There are some simple steps that you can take to increase your security and ensure that even though you got pwned, you don't get hacked.

But first, let’s take a moment to understand the actual threat here. Your email address is one among millions, billions. How concerned do you need to be? To answer that question, let’s examine…

How do attackers use breach data?

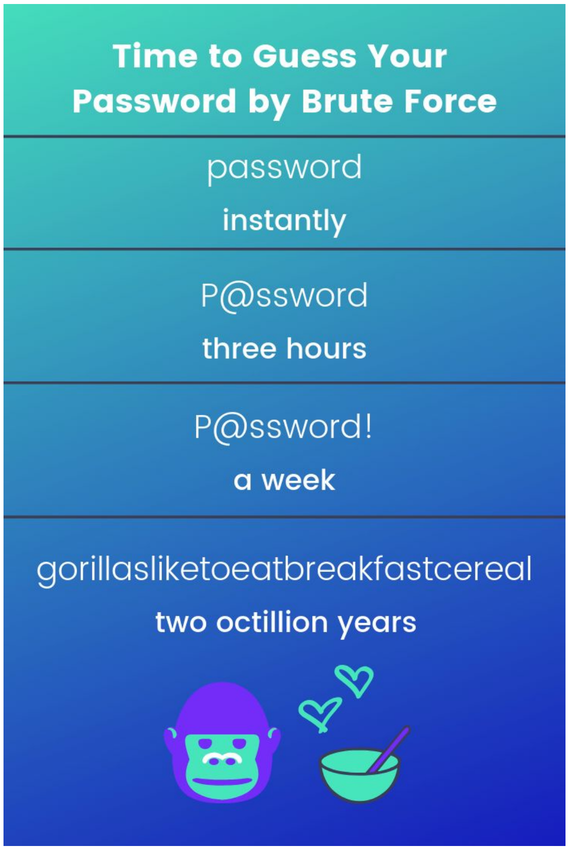
Attackers use account and personal data released in these types of breaches to attempt to gain access to other user accounts. For instance if your LinkedIn email address and password were leaked, it’s not only your LinkedIn account that could be compromised. If you use that same email and password for your bank account or any other account, an attacker could gain access to that using your stolen LinkedIn credentials. This type of attack — attempting to log into a variety of accounts using leaked email/password pairs — is called “credential stuffing”. That’s why it’s really important to ensure that you use a different password for each account.

Even if your password data was not included in the breach, attackers can do similar guesswork by attempting to log into various websites using your email address combined with the most common passwords from other breaches that may not have even included your accounts. Attackers typically aren’t going through these email/password combinations one by one. They use bots and computing power to mass attempt log in with usernames and passwords in bulk across a variety of sites. That’s why it’s important to use strong passwords that are difficult for both humans and computers to guess.

So the first step in making sure this breach doesn’t result in you getting hacked: change your passwords for all accounts under your “pwned” email address to strong and unique passwords.

When changing passwords, be sure to use unique passwords for each account. You might be wondering how in the world you’ll be able to remember all those passwords. The good thing is that you don’t have to remember each and every one of these. Let technology do the remembering for you and use a password manager. If you already use a password manager, great! If you don’t, two reliable ones are Lastpass and 1Password. Password managers allow you to only remember one secure password! You can then securely store, share, and change your other passwords. Some of these services even have password generators that take the thinking out of creating a strong password.

Why password strength matters



Time to Guess Your Password by Brute Force

password

instantly

P@ssword

three hours

P@ssword!

a week

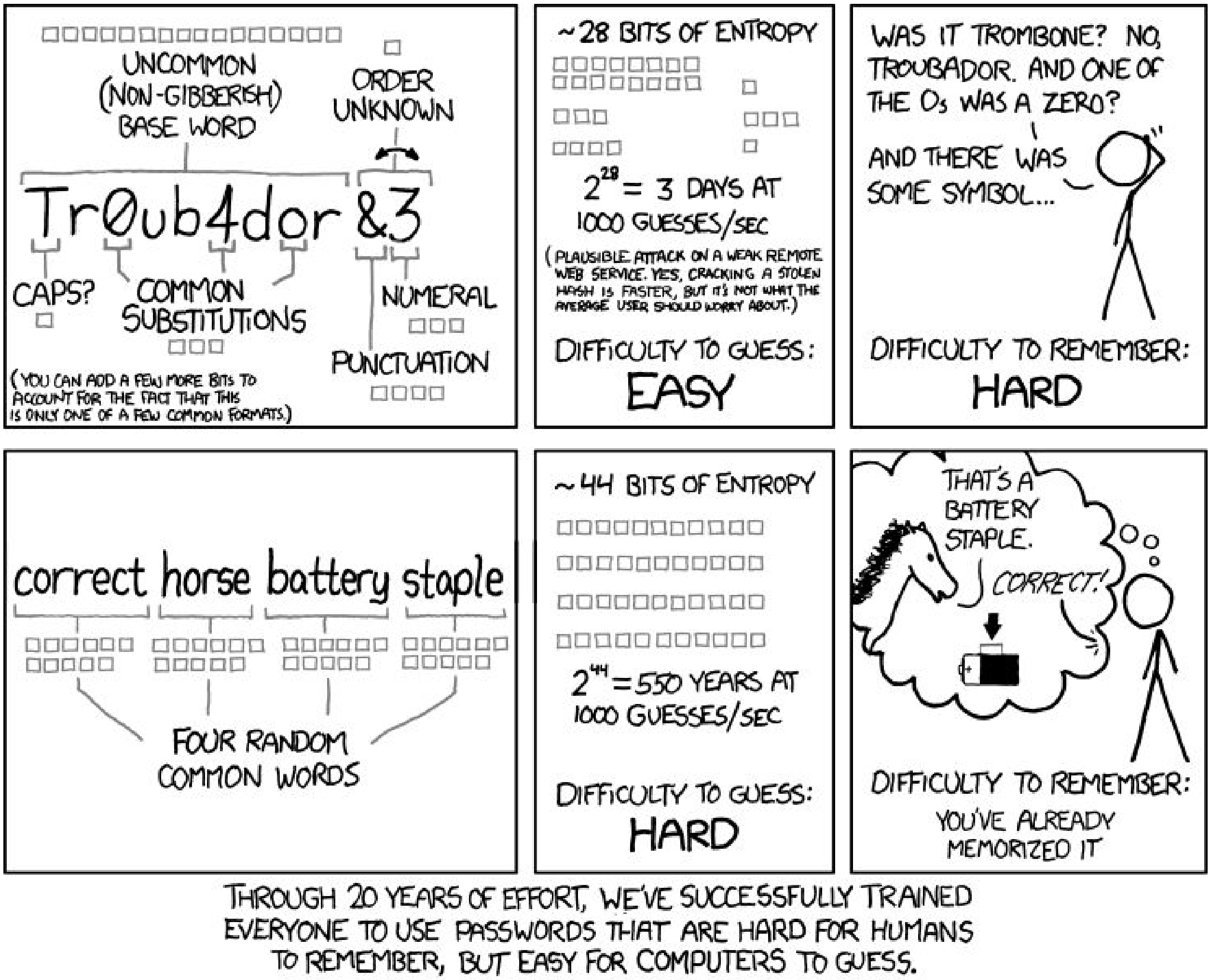
gorillasliketoeatbreakfastcereal

two octillion years

Length of time it would take a computer to guess a variety of passwords.

Aside from being unique per account, your newly changed password should be longer than eight characters and include a variety of different characters. A strong password will not contain any easily guessable items like your birthday, names of pets or family members, etc. Not including personal data in your password protects it from being guessed by a human. To ensure that your password will also be difficult for a computer to guess, you can use https://howsecureismypassword.net/. This service calculates how long it would take a computer to guess or ‘crack’ your password by ‘brute force’ attack (attempting permutations of character combinations until log in works).

This isn’t the only way people can use computing power to try to crack your password. They can also set up bots to check the top 10,000 passwords – which is why we wouldn’t recommend using ‘P@ssword!’, even though it’s better than ‘password’. Bots can also run a dictionary attack, where they try every word in the dictionary, so a password that combines multiple words will always be your best bet.


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Strong, unique password? Check!

Great, so you’ve changed all your passwords to super strong, super unique passphrases of beauty that would be practically impossible for an attacker to guess by brute force… but you forgot to change one account.

Let’s say the worst case scenario occurs, and attackers are able to correctly guess the email/password combination to gain access to that one account you forgot to update.

Is all hope lost? Are you doomed? Now do we panic? Not so fast! If you have two-factor authentication enabled for your account, your password is not enough information to get into your account, so your account will be protected.

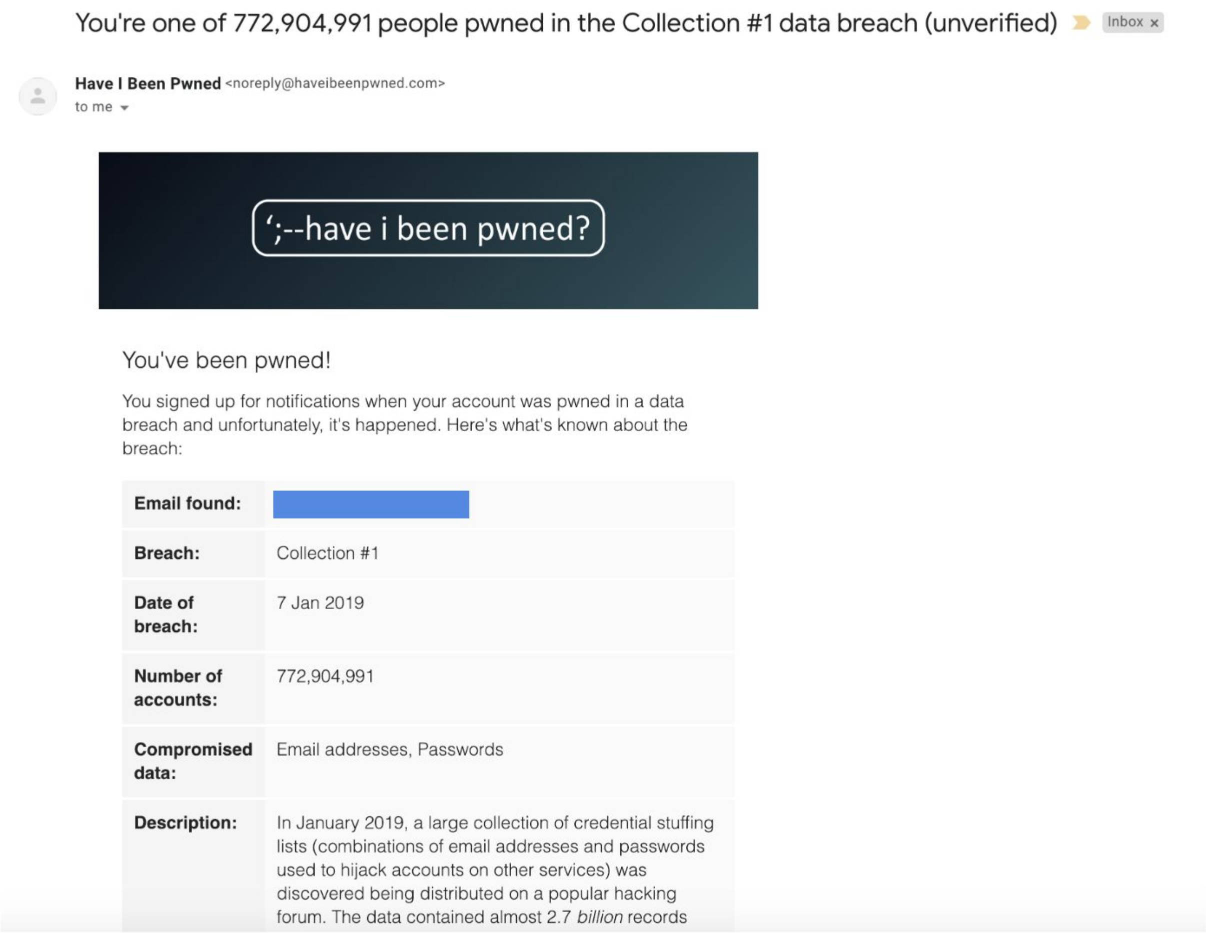
Step two in ensuring this breach doesn’t result in you getting hacked: enable two-factor authentication on all accounts.

Two-factor authentication (2FA) essentially means that your email + password are not the sole line of defense to your account. The two factors we like to use are “something you know,” (your password) and “something you have.” With 2FA, your phone (or a physical key such as a yubikey) can be the “something you have” used to verify that it’s actually you who’s signing into your account.

In the scenario above, instead of an attacker getting into your account, you’d receive a text message with a code to continue logging into your account. This would alert you to the fact that somebody else was trying to gain access to your account and knows your password.

How can I be notified if I’m affected by future breaches?

Sign up for email alerts from “have I been pwned?” ! In the event of any future breaches, you’d receive an email like the one below:



You're one of 772,904,991 people pwned in the Collection #1 data breach (unverified)

Have I Been Pwned <noreply@haveibeenpwned.com>
to me

You've been pwned!

You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Email found:	[redacted]
Breach:	Collection #1
Date of breach:	7 Jan 2019
Number of accounts:	772,904,991
Compromised data:	Email addresses, Passwords
Description:	In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 *billion* records

Take a moment to pat yourself on the back for learning how to secure your accounts! If you are able to take the above steps, you'll be in great shape to deal with any fallout from the current breach as well as prepared to take on future breaches. The threat of data breaches isn't going away, but with a little bit of preparation, you can sit back and relax, just like this cute sloth in a hammock.

Sloth who uses strong, unique passwords, a password manager, and 2FA on all accounts.

If you're an abortion access organization and you have further questions or concerns about third party data breaches and what they mean for your organization, please send us a note on our contact page. We're here to help!